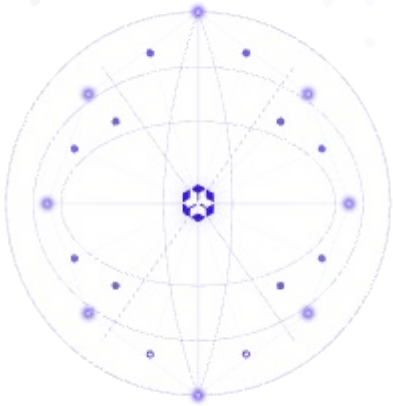
ASTRAN



Workshop

When the CISO meets the Head of Treasury to build Operational Resilience

April 1, 2026

Executive Summary

Resilience is everyone's problem, starting with the Executive Committee.
Resilience cannot be delegated to IT or Business teams alone. Without Executive Committee-level (or even Board-level) ownership and cross-functional co-governance, resilience programs fail to gain traction when it matters most. Executive sponsorship is not a nice-to-have, it is the single most critical enabler.

Vital Activities must be defined top-down - and they are not a BIA.
Identifying what the company must preserve at all costs is a strategic decision. Unlike a Business Impact Analysis that is a useful bottom-up approach to discuss with every team internally, Vital Activities require leadership to make deliberate choices about what the organization is willing to let go of in a crisis, and what it absolutely cannot.

Treasury must brings its business and process expertise to the table.
Sitting at the end of every financial chain yet touching every Business line, Treasury is uniquely positioned to map critical processes, build payment simplified processes and stress-test the company's financial continuity.

The CISO must act as resilience leader by addressing the wake-up call regarding cyber interruption riks and coordinating the company-wide resilience effort.
Cyber's most powerful contribution is honesty: a full IT shutdown lasting several weeks (24 days in average*) is not a theoretical worst case, it is a realistic one. CISOs must help the organization Businesses and the Executive Committee understand the real scenario of a cyber interruption, and coordinate the Resilience effort.

Industry context: average downtime of 21*-24** days (Coveware*, Statista**)

Overview

This workshop brought together 15 Treasury and Cyber-Resilience Leaders to explore how organizations can build a robust Resilience Strategy through cross-functional collaboration. They focused on key questions: who should own Resilience within the organization, what should be considered as Vital Activities, and what Treasury and Cyber teams can each bring to build the Minimum Vital Company.

Resilience Ownership

The group was divided, but a clear consensus emerged around one principle: resilience cannot sit in a single silo. The Executive Committee and a co-ownership model were equally favored, reflecting a shared belief that Executive Committee-level (or even Borad-level) sponsorship is the single most critical enabler. Without it, Resilience programs struggle to gain traction across the organization.

What should be considered as Vital Activities

Vital Activities represent a handful of business outcomes an organization must preserve, no matter what. The MVC framework structures these around five universal categories, and the workshop responses mapped closely onto them:

Keep the Core Service running - production, supply chain, ERP, R&D.
Participants emphasized the need to identify which production lines or service flows are truly existential, and which can be temporarily suspended without threatening survival.

Be able to make Critical Payments - debt service, supplier and payroll payments, treasury operations.
This was the second most discussed category. Debt service in particular was flagged as a recurring concern: its disruption triggers a dangerous snowball effect, making refinancing nearly impossible, eroding confidence and driving up rates.

Customers get served and monetized - sales, ecommerce, client delivery.

People and Sites stay protected - product and people safety, crisis processes.

The company communicates and stays compliant - brand reputation, regulatory response, investor and partner updates.
In crisis, silence creates speculation; inconsistent communication creates mistrust. Brand image was flagged as particularly vital in luxury and consumer-facing sectors, where a non-functional point of sale is simply not an option.

The group emphasized that within each Vital Activity, organizations should define a minimum threshold, and be ready to prioritize one critical element over others when survival is at stake.

What can Treasury/Cyber bring to the MVC

Treasury

Treasury's contribution was seen as uniquely cross-cutting. As a function that sits at the end of the chain yet touches every Business line, Treasury is well positioned to map and prioritize critical processes, build payment simplified processes, list and protect critical data, and help identify needed assets. Its business expertise (including RETEX from past incidents) and strong banking relationships, makes it a natural co-owner of the MVC.
The key message: Treasury's role is to "lay the risks on the table clearly" and work with other functions to make deliberate choices.

Cyber

Cyber's most valuable contribution is its honesty and expertise, knowing which applications are truly critical, preparing for worst-case scenarios, and bringing cross-functional crisis management experience. Participants also emphasized Cyber's role in validating backup solutions, defining RTO/RPO, securing fallback environments, and educating the company and Executive Committee on the realistic magnitude of a cyberattack: a full IT shutdown lasting several weeks is not a theoretical scenario.

Key Takeaways

- Anticipation is the defining word for Cyber Resilience
  Organizations that haven't done the upstream work won't hold when a crisis hits. A solution must be designed and validated before the incident occurs
- Crisis exercises are the most effective awareness tool
- Fraud risk spikes during a crisis, making strict internal audit and controls non-negotiable during response and recovery phases
- Finally, a framing from researcher Olivier Hamant resonated with the group: Resilience should be understood as robustness over performance. In his work, Hamant shows that living systems survive not because they are optimized, but because they are robust - a useful lens for any organization building its continuity strategy.

The MVC framework highlights that **Resilience is not about maintaining everything, it is about ensuring that what truly cannot stop, does not**. The workshop confirmed that Treasury and Cyber, when aligned around a shared set of Vital Activities and brought together under Executive sponsorship, are two functions well positioned to make that promise operational.